Chapter 13

Watermarking for Still Images Using a Computation of the Watermark Weighting Factor and the Human Visual System in the DCT Domain

O-Hyung Kwon
Sogang University, Korea & ETRI, Korea

Rae-Hong Park
Sogang University, Korea

ABSTRACT

In this chapter, the authors propose a Discrete Cosine Transform (DCT)-based watermarking method using the calculation of the watermark weighting factor and the Human Visual System (HVS) for the given peak signal to noise ratio of still image as well as the specified length of watermarks to be inserted. Using the energy relationship of the DCT, they derive the equation that directly computes the watermark weighting factor in the DCT domain. In addition, the authors propose a digital watermarking method for still images, in which the HVS is used in the DCT domain. The modulation transfer function of the HVS model is employed to increase the invisibility of the inserted watermark in images. Experimental results show that the proposed watermarking method is an effective objective evaluation method to compare the performances of watermarking algorithms.

DOI: 10.4018/978-1-4666-2217-3.ch013
INTRODUCTION

Recently, a huge usage of video on demand services and social network services has increased the commercial potential of providing multimedia resources through various digital networks such as the Internet. However, it is possible to illegally copy and transfer the digital multimedia to others through the Internet. To prevent this, the digital watermark methods were suggested (Vahedi, et al., 2012; Jayanthi, et al., 2011; Patra, et al., 2010; Cox, et al., 1996; Craver, et al., 1998; Barni, et al., 1997; Pitas, 1998; Motwani, et al., 2010). The owner of the digital image or video can insert his/her own particular signal (watermark) into digital image or video to insist ownership, where the watermark can be a random number with a specific seed number and size or a specific code identifying the owner. If a malicious user gets and transfers this image or video to others, the owner can extract the watermark, which has been inserted into the image or video using a specific watermark method and can insist the ownership who is the real owner of that image or video. The encryption techniques have been used to protect illegal reproduction of the digital multimedia. However, the piracy problem could not be solved perfectly by this method because nobody can insist copyrights or ownership of the decrypted digital multimedia contents. To solve this problem, many digital watermarking techniques have been studied to protect the ownership of the digital contents (Cox, et al., 1996, 1997; Cox & Miller, 1997; Craver, et al., 1996, 1998; Barni, et al., 1997; Pitas, 1998; Piva, et al., 1997; Kwon, et al., 1999, 2006). The digital watermarking is an information hiding technique to insert secret data into the original contents. The secret data that is information including an ownership can be easily extracted from the watermarked digital multimedia contents and it can be decided who the right owner of the watermarked digital contents is. The main requirements of digital watermarking methods to protect the copyright of a digital image or video are:

- Watermarks cannot be distinguished visibly after inserting it into original image or video
- It is impossible to statistically detect the watermark information
- Watermarks can be detected after general signal processing
- Watermarks can be extracted even under malicious attacks (Cox, et al., 1997)

The digital watermarking methods can be categorized into text watermarking, still image watermarking, video watermarking, and audio watermarking according to where watermarks will be inserted. The digital watermarking method can satisfy the requirements mentioned above and there are two kinds of watermarking methods for still image watermarking to satisfy those requirements: one is to insert watermark in the spatial domain and the other in the frequency domain. Watermarking methods in the spatial domain have a merit that the watermark can be inserted and detected easily. Frequency domain watermarking methods have been studied because they are more robust than the spatial domain watermarking against several malicious attacks and noise.

A method was proposed, in which the identification string was inserted in digital audio signals by substituting Least Significant Bit (LSB) of audio samples with identification bit strings (Schyndel, et al., 1994). The LSB of insignificant bit means the smallest audio signal level that human can hardly distinguish. This method was applied to two-dimensional (2-D) still image, however it turns out that this method has a drawback of easy forgery.

Caronni proposed a method by inserting the geometrical patterns into the quantized luminance level that can be hardly distinguished visibly (Caronni, 1995). However, the method of insert-
Related Content

Socio-Economic and Environmental Impacts of Poor Paper Management at Higher Education Institutions in Ethiopia: Evidence From Hawassa University

Malware Detection and Prevention System Based on Multi-Stage Rules

The Compliance of IT Control and Governance: A Case of Macao Gaming Industry
[www.igi-global.com/article/the-compliance-of-it-control-and-governance/155103?camid=4v1a](www.igi-global.com/article/the-compliance-of-it-control-and-governance/155103?camid=4v1a)

[www.igi-global.com/article/cloud-risk-resilience/227022?camid=4v1a](www.igi-global.com/article/cloud-risk-resilience/227022?camid=4v1a)